PER144
FOR DECISION
WARD(S): GENERAL

STANDARDS COMMITTEE

7th April 2008

PERSONNEL COMMITTEE

3rd March 2008

IM&T SECURITY AND CONDUCT POLICY

REPORT OF THE HEAD OF IM&T

Contact Officer: Sheila Davidge Tel No: 01962 848262 Email: sdavidge@winchester.gov.uk

RECENT REFERENCES:

None

EXECUTIVE SUMMARY:

The current Computer Security Policy and Conduct was published in November 2002. The Policy had been supplemented by improved security of data and network security for access to Government Connect.

The Policy has been made more explicit and clearer in certain areas, particularly in relation to matters that may be considered gross misconduct that would warrant termination of employment for staff without notice. The Policy also now applies quite expressly to Members.

Government Connect (GC) is a national secure network that is being rolled out to all local authorities and in use within central government. We are working with Hampshire County Council, who will host the network link and other partners within Hampshire to roll out GC. GC entails major improvements to the network security which has required upgrades to hardware and software to ensure that we meet the very strict conditions.

The Council need to comply with Payment Card Industry (PCI) Data Security Standards and the upgrades mentioned above will help comply with these standards.

It is important that a robust Policy exists, is up to date and is disseminated to staff and Members so that any disciplinary action to be taken by Management or the Standards Committee is supported appropriately. New staff will be told of the Policy at induction sessions. Existing staff will be told of the Policy through the City Voice, it will be published on the Intranet and briefing sessions will be organised. GC requires that we record acceptance of the policy by all staff and Members and a process will be set up to comply with this requirement.

Briefing for Members will be arranged as part of one of the future training sessions already programmed.

RECOMMENDATIONS:

1. That Members approve the attached IM&T Security and Conduct Policy.

OTHER CONSIDERATIONS:

1 CORPORATE STRATEGY (RELEVANCE TO):

1.1 The report accords with the tenet of make best use of resources.

2 RESOURCE IMPLICATIONS:

2.1 There are no direct resource implications in approving the revised Policy. Indirectly, the Policy aims to achieve more efficient use of resources and to protect the Council from loss or additional cost.

BACKGROUND DOCUMENTS:

Working papers held within IM&T

APPENDICES:

Appendix A: IM&T Security and Conduct Policy

INFORMATION MANAGEMENT AND TECHNOLOGY (IM&T)

SECURITY AND CONDUCT POLICY

Information Management and Technology (IM&T)

Security and Conduct Policy

1 Aims of the Policy

1.1 This policy document establishes the IM&T Security and Conduct policy for Winchester City Council (the Council) to safeguard information and processes associated with electronic information and communication systems. This Policy also assists in promoting computer security awareness within the Council and encouraging reasonable and well-informed behaviour as well as good management practice.

1.2 This policy is designed to:

i) Safeguard information, processes, behaviour and conduct associated with electronic information and communication systems both within Council policy and the wider legislative framework.

ii) Assist in promoting computer security awareness within the Council, maximising the advantages that Internet and e-mail access bring whilst seeking to minimise the associated legal risks and practical hazards.

iii) Encourage reasonable and well-informed behaviour as well as good management practice. The Council's policy is for members and staff to be familiar with the Internet, e-mail and other electronic facilities at their disposal so that confident, skilled users are developed.

1.3 Any breach of this Policy by staff may lead to disciplinary action being taken and, in cases of gross misconduct, termination of employment. Any breach of this Policy by Members will be referred to the Standards Committee. Any breach of this Policy by contractors will be subject to appropriate action by the relevant Head of Division.

2 Scope

2.1 This Policy applies to all Council personnel, temporary/agency staff, contractors, consultants, suppliers and Councillors who use any Council information or communication technology, whether these systems are being used on site or away from Council premises.

3 Infringements of Policy

3.1 Infringements of this Policy will warrant disciplinary action and, in cases of gross misconduct by staff, termination of employment without notice. In particular, attention is drawn to the following infringements:

3.2 Viewing, creating, circulating, distributing, storing, downloading or printing material that might be offensive, illegal, pornographic or sexually explicit, that brings the Council into disrepute or that exposes it to legal action. For staff, such action is likely to be considered as gross misconduct and, if so, would result in termination of employment without notice. The Council reserves the right to recover defamatory material and use it as evidence against an individual.

ii) Using communication facilities for purposes that may be illegal or contravene Council policy such as disclosing official information without authority.

iii) Hoaxing, hacking or damaging Council or other networks, or knowingly using unlicensed software.

iv) All staff emails must not be sent without prior approval of IM&T or the Head of Division, Director or Chief Executive.

v) Using communication facilities (landline, mobile or email) for unreasonable extensive private use contrary to the provisions of the guidance given in paragraph 15 of this Policy

vi) Passing any personnel information of a member of staff or member of the public to any other individual not related to the business of Winchester City Council.

vii) Not complying with the Council's policy on electronic document management when it is introduced.

4 Responsibilities

4.1 **All users** are responsible for ensuring that they comply with this Policy. A pop-up box appears at logon stating that, by logging on, users agree to accept the terms and conditions of this Policy when entering the Council's network.

4.2 Under Government guidelines all users of the network will be required to sign a document stating that they have read and understood the Information Security Policy. Where possible this will be carried out electronically on a six monthly basis.

4.3 The Head of IM&T will:

i) Review this Policy annually, in consultation with the Head of Organisational Development.

ii) Develop and publicise this Policy and inform end users of IM&T security issues.

iii) Develop administrative, physical, and technical security controls to meet the Council's IM&T security objectives including allocation of passwords and security of remote dial-in mechanisms.

iv) Monitor use of the Internet and email and access to any computerised device using the Council's network, whether owned by the Council or not.

v) In co-operation with the relevant Head of Division, perform periodic risk analyses to identify potential information or data losses and the effect of such potential losses.

4.4 The Head of Organisational Development will:

i) Provide a copy of this Policy within the Induction Pack issued to new staff.

ii) Ensure that induction training courses outline the key elements of this Policy, provide general guidance on the use of electronic systems and cross-reference with the Council's Equal Opportunities Policy.

iii) Provide IM&T & IT Contractor with a list of Starters at least two weeks before their start date, of Leavers at least one week before their last working day and of staff changing duties at least one week before the change takes place, so that user information is kept up to date,

iv) IM&T to be advised of any member of staff who has been given permission to work from home or be a mobile or nomadic worker.

4.5 Heads of Division will ensure that:

i) This Policy is transmitted to all staff, contractors, consultants and agency staff within their Division and to all Members.

ii) The procedures within this Policy are complied with and appropriate security measures are established and maintained with regard to access to Council databases and other electronic information systems or resources.

iii) IM&T & IT Contractor is informed of the details of systems which Starters can have access to two weeks before their start date and of details of staff transferring duties two weeks before the due date and of Leavers at least one week before their last working day.

iv) IM&T is advised of any members of staff who have been given permission to work from home or be a mobile or nomadic worker.

5 Security - Monitoring of System Usage

5.1 The purpose of monitoring is to:

i) Monitor personal use of e-mail and Internet services that may be costly and can affect the efficiency of the network system as a whole.

ii) Monitor security issues such as disclosure of information or accessing unreliable sites with a risk of virus or unsuitable sites or excessive use.

iii) Ensure usage of the systems does not disrupt or damage the performance or reputation of the Council.

5.2 The Council will monitor the use of all of its IM&T equipment, in particular the use of the Internet and the contents of mail and file transfers, irrespective of whether they are for Council or private use. Internet monitoring shows which sites are accessed, by whom, when and for how long. This evidence may be used during a disciplinary investigation.

5.3 Monitoring reports will be made available to Heads of Division who are responsible for taking appropriate action. Where necessary the Head of IM&T, the Head of Organisational Development, Corporate Director (Governance) or the Chief Executive will advise on the suitability of material, investigate web sites or seek the opinion of the police.

5.4 The Council reserves the right to access data files held within personal folders or password protected files in connection with the legitimate business of the Council.

5.5 The content of e-mails (both incoming and outgoing) will only be accessed where specific circumstances justify this action. All such monitoring will be carried out for legitimate purposes only and in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Monitoring will take place on a monthly basis and Heads of Division will be provided with this information and which they will act upon as appropriate.

6 Hardware and Software

6.1 All IM&T hardware will be registered, when procured, with a unique asset number recorded on the Council's asset register.

6.2 Users should not move PCs, printers, scanners or other IM&T equipment as this must be done only by the Council's IT contractor.

6.3 No hardware, such as peripherals or laptops, should be connected to the Council's network without the permission of IM&T.

6.4 Good management procedures must be followed in relation to all equipment. Specifically:

i) Council-owned portable PCs and computer accessories must be stored in a locked cabinet when not in use, except when kept at home.

ii) A signed record, including the asset register number, must be held within the division for borrowed portable computer equipment.

iii) Any sensitive data saved on the hard drive must be removed or deleted by the user when portable equipment is returned.

6.5 The disposal of surplus and obsolete IT & telephone equipment must be through IM&T.

6.6 All software packages used on Council owned, leased or rented computer systems, including copyrighted freeware and shareware, must be registered prior to installation in the Council's Inventory managed by IM&T.

6.7 Users must observe copyright and licensing agreements. Software is usually licensed only for a particular number of users. If anyone is unsure how many copies of software are licensed for their use, the onus is on the individual to ensure that they are using licensed software. Advice on licensing may be sought from IM&T. Licensing agreements vary and individuals are responsible for understanding and abiding by the terms.

6.8 No software should be loaded on Council equipment except by the Council's IT contractor, after it has been purchased or obtained by IM&T and with the approval of the appropriate Head of Division.

6.9 No software should be downloaded from the Internet except by the Council's IT contractor. It must be virus scanned before it is loaded and used. All licensing requirements, payment conditions and deletion dates associated with downloaded software must be met. Anyone requiring software must be aware of the differences between: copyrighted software (which requires a licensed payment); free ware (which is licensed but requires no payment); shareware (which is copyrighted but often free for a trial period), and public domain software (which is free). Guidance should be obtained from IM&T.

6.10 All software, hardware and electronic equipment must be purchased through IM&T who will ensure licensing agreement forms are filed with the supplier. Registration may provide the basis for getting assistance from the manufacturer if the software is lost, stolen, or damaged.

6.11 Staff must use only those electronic resources that have been authorised by their manager. The use of Council equipment for unlawful purposes, including the installation of fraudulently or illegally obtained software, is strictly forbidden and will lead to disciplinary action being taken.

6.12 Users must switch off PCs, screens and printers when going home or when leaving them unattended for some time.

6.13 Multi Functional Devices must not be switched off.

6.14 The computer suite must be locked and access through a key pad that is changed every 30 days. Any access to the computer suite should be recorded and monitored by the IM&T Client Officer.

6.15 When a member of staff leaves the employment of the IT contractor, the password must be changed immediately and the IM&T Client Officer informed. All system passwords must also be changed.

6.16 All systems must be backed up by the IT Contractor in agreement with the IM&T Client Officer. All backups MUST be stored offsite in a secure location.

6.17 The spare keys used by the IT Contractor for fire safe, cabinets etc, must be stored in an offsite location.

7 Working from Home/Mobile Working

7.1 Additional arrangements apply to staff using Council IM&T equipment or services from home or when mobile.

7.2 Laptops and other portable devices:

i) Must not be left unattended in public places

ii) Must not be left in a car overnight

iii) Must be kept in the locked boot of the car and out of sight when left unattended at other times.

iv) Must be carried as hand luggage

v) Must be protected from exposure such as to impact; strong electromagnetic fields; extremes of temperature; spillages of food or drink

7.3 Use of Council equipment is restricted to Council business only unless permission is given from the Head of Division and appropriate tax is paid to Revenue and Customs.

7.4 If personal equipment is used to access Council services care must be taken to ensure that viruses are not spread. Virus checking software must be installed, be updated weekly and it must always be active.

7.5 Data accessed from home or when mobile should be treated with the same confidentiality as data accessed in the office. Equipment and data should not be left unattended.

7.6 Those working from home should familiarise themselves with the Council's Working from Home Policy.

8 Data and Files

8.1 Physical access by non-authorised personnel to the Council's electronic equipment is strictly forbidden.

8.2 Unattended computer terminals must be password protected either by being at a logon prompt or by a password protected screen saver.

8.3 All employees must be alert to the presence of non-authorised personnel in the vicinity of computer equipment.

8.4 All files must be stored on a server and items downloaded to a laptop for a specific reason must be uploaded to the server if any changes to documents or information and earlier versions deleted from the hard drive.

8.5 Personnel information must not be saved on hard drives or external devices (i.e. USB or CD). Data must not be stored on local drives.

8.6 Particular care must be used when working on confidential or sensitive information. Such files should be kept in a secure directory on the server that will need the author's login for access. Any paper with sensitive information must be locked in a secure cabinet when not being used.

8.7 Any personal data being shared with a third party should either be encrypted or password protected and the password sent in a different document than the actual document. Advice on encryption and password protection should be requested from IM&T. Care should also be taken to comply with data protection principles in the Data Protection Act. Sharing of personal data should always be approved by the individual's line manager. Advice can be obtained from the Legal Division and IMT.

8.8 In future, when the connection is available, any sensitive information should be emailed via Government Connect (Gateway).

8.9 Reports and customer data should not be left lying around where unauthorised access may be readily available.

8.10 Data accessed from home should be treated with the same confidentiality as data accessed in the office.

8.11 Unauthorised access to data and files (Hacking) is forbidden.

8.12 Large files should be reviewed prior to saving on the main servers. i.e. photographs should be reviewed prior to being saved and unwanted photographs deleted.

9 Passwords and Logons

9.1 All users of any Council computer system must be issued with an individual password and logon.

9.2 Users must adopt sound password practices:

i) Passwords must be kept secret and must not be disclosed to others.

ii) Passwords should not be recorded unless the record is stored securely.

iii) Passwords disclosed to another individual must be changed immediately.

iv) Passwords should not be saved and option boxes for saving passwords should not be checked (ie not ticked).

v) User Passwords must be changed every 60 days and main system passwords every 30 days.

vi) Passwords should be a minimum of eight characters and must contain at least three of the following characters: upper case, lower case, digits and symbols (unless there are system constraints).

vii) Passwords cannot be reused for twenty changes.

vii) If temporary passwords are required these must be changed or deleted as soon as possible.

ix) Temporary passwords must be conveyed to users in a confidential manner.

x) Passwords should not be based on the following:

- Family names, initials or car registrations.
- Months of the year, days of the week or any other aspect of the date, company names, identifiers or references.
- Telephone numbers or similar all-numeric groups.
- User ID, user name, group ID or other system identifier.
- More than two consecutive identical characters.
- All numeric or all-alphabetic groups (unless the system requires it).

9.3 Users must use only their own user name and password to access any system.

9.4 Users must not allow anyone else to use their user name and password. This is not only a security risk but could lead to false accusations of misuse as monitoring of the Council's Internet usage is based on user names.

9.5 Users must not attempt to find out the password of another user.

9.6 Outside suppliers dialling in remotely to the Council's network to support applications are not required to have individual user names and passwords but must complete a Change Control form which is authorised by IM&T Client Officer.

9.7 A corporate screen saver should be activated after 15 minutes and users must enter their password to unlock the screen.

9.8 Where laptops are used for home logons the password file must not be saved (ie the dialogue box indication to save the password should not be activated) in order to prevent unauthorised access if the laptop is lost or stolen.

9.9 Further security for laptops and staff working from home or mobile will be implemented using 'key fobs' which provide a unique number and is used as part of the login procedures. If any 'key-fob' is lost or

misplaced this must be reported to IM&T Client Officer immediately. Access to the Network will not be possible without the 'key-fob'.

10 Security Incident Reporting

10.1 Any user who feels their password security has been compromised should change their password immediately and report the incident to IM&T.

10.2 Any user who feels that malicious damage may have been caused by someone using their user name and password should report the incident immediately to their Head of Division and IM&T.

11 Computer Viruses

11.1 All mail is filtered by a third party anti-virus, spam and content filtering software solution and anti-virus software is running in the background on all Council PCs.

11.2 Users should ensure that they are aware of the nature and danger of computer viruses and should take all care to ensure that they are not introduced to the Council's computers or its networks.

11.3 There are two types of viruses. A benign virus may simply flash an annoying message on the screen, whilst a malicious virus may destroy information. Viruses are most frequently spread via the downloading of files from the Internet, through the use of an infected USB or CD or by attachments to email messages.

11.4 The use of floppy disks, USB's and CDs are restricted, approval for the use of such devices must be agreed through a business case by Heads of Division and IM&T

11.5 To reduce the chance of getting a virus, users should virus check all USB's and CDs before use. Software should only be downloaded from the Internet by the Council's IT contractor. **ALL suspected viruses must be reported to IM&T immediately.**

11.6 Heads of Division are responsible for ensuring that the Council's anti virus software is not removed from the PCs in their division.

11.7 Any information about virus warnings should be given to IM&T who will check the information and issue a message to all users if appropriate.

11.8 Users should be cautious about opening email from an unknown source and should not open attachments to such emails. Any suspicious emails should be referred to IM&T.

12 Hoaxes

12.1 There are many virus hoaxes that claim falsely to describe an extremely dangerous virus. They use pseudo-technical language to make impressive-sounding, but impossible, claims. They claim that

the report was issued or confirmed by a well-known company and ask you to forward it to all your friends and colleagues.

12.2 Users must not pass on warnings of this kind, as the continued re-forwarding of these hoaxes simply wastes time and email bandwidth.

12.3 Hoaxes via email may come with a file attached. Such attachments should be treated with caution as they may be infected with a virus. Any user found to have distributed hoax information intentionally via any Council communication system will be subject to disciplinary action.

12.4 Other hoaxes that are scams designed to deceive people into parting with money also circulate. Users should be vigilant and pass any suspected hoax e-mails to IM&T who will investigate and issue a warning as appropriate to all staff and councillors.

13 Conduct - General Use of Equipment

13.1 The Internet, use of e-mail and text messaging now has a substantial presence throughout the world. As a consequence of e-mail, Internet and other electronic activities, defamation and harassment action, negligence cases, breaches of copyright and claims in respect of disclosure of trade secrets and personnel information have arisen.

13.2 Council electronic equipment and software should be used in a responsible, legal, and ethical fashion. Users must not take any action that could bring the Council into disrepute, cause offence, interfere with Council work or jeopardise the security of data, networks, equipment or software.

13.3 Council computer equipment and software, as well as telecommunication services and other electronic equipment are for Council business purposes. Occasional personal use by staff is permitted at the discretion of line managers provided it does not interfere with Council work, is not conducted in Council time, conforms to this Policy and is not associated with personal business interests. Similarly, Members may use Council equipment for occasional personal use and for Council and ward matters. However, Council equipment must never be used to promote support for a particular political party nor for conducting personal business interests. Council equipment must only be used by council employees or members.

13.4 Those who use their own PCs or other equipment to connect to the Council's network remotely and who use that connection in contravention of this policy will face disciplinary action in the same manner as those using Council owned equipment.

13.5 The removal of Council owned software and hardware for personal use, whether done by copying or by removal of the master software, is prohibited and illegal under the Council's contracts with the vendors.

14 Workstations – Health and Safety

14.1 Risk assessments must be carried out within each Division on workstations used by staff. Help on this can be obtained from the Council's Health and Safety Officer.

14.2 Users should ensure they are familiar with the Council's policies on Health and Safety with regard to workstations, either in the office or at home.

15 Messaging (Telephone, mobile and email)

15.1 Messaging means communications made by email and telephones, including mobile phones, and includes text and media messaging.

15.2 Messaging, whether sent internally or via the Internet, should be regarded as public and permanent. It is never completely confidential or secure and, despite its temporary nature, it can be stored, re-sent and distributed to large numbers of people.

15.3 Messaging must not be used for sending offensive, threatening, defamatory or illegal material. Messaging can be the same as sending a letter or publishing a document in law, so defamatory comments could result in legal action.

15.4 Managers should be particularly careful what they commit to messaging. It can be used as evidence in industrial tribunals and formal enquiries, including internal disciplinary and grievance hearings.

15.5 It is poor practice to use messaging to criticise or rebuke staff. Such matters should only be discussed face-to-face.

15.6 Messaging must not be used to harass staff or other recipients. Harassment can take the form of argumentative or insulting messages (flame mail) or any other message the sender knows or ought to know would cause distress to the recipient.

15.7 Users posting information to newsgroups should not include any information that brings the Council into disrepute or that promotes support for a particular political party. Including a disclaimer may not be sufficient.

15.8 It is easy to be misunderstood in messaging. People forget that the emotional meaning is often lost in text. Humour can be misinterpreted. Email and text messaging should be unambiguous. Neticons (symbols such as ☺ used to show humour, sadness or anger) are not widely understood and should not take the place of a clear message in plain English.

15.9 Every user has a mailbox limit - that is, there is a restriction on the volume and size of e-mails that can be held in Received, Sent and Deleted boxes. Each user should maintain good housekeeping arrangements by deleting e-mails frequently in each of these areas or by saving them to either their filing structure on the server or within

the EDRM (Electronic Document and Records Management system). If housekeeping is not carried out the user will receive a message warning them that their limit is being reached. In some cases e-mail may not be received or sent until housekeeping is done. If this causes problems IM&T should be contacted.

15.10 To reduce the problems associated with mailbox limits, users should refrain from sending large files, such as those which contain graphics, such as logos and electronic signatures. In addition to causing problems with both their mailboxes and the recipient's, transmission of large files can slow down the network and impede the work of others.

15.11 The email and telephone system is for business communication: thus personal messages unconnected with work should be kept to a minimum. The Council expects all members and staff to adopt a common sense and reasonable approach to the use of such facilities. Staff should conduct any personal messaging in their own time.

15.12 Personal use of the Council's messaging systems is permitted for exceptional reasons such as an immediate need to contact the emergency services, or in the case of a domestic emergency, for example a family illness or changes to carer responsibility arrangements. Such messages should be kept to a minimum and wherever possible be carried out in the staff member's own time.

15.13 Staff are not permitted to use the telephone system for international or high rate premium number calls.

15.4 Those with Council mobile phones should arrange to have a second line connected for personal calls. Personal calls or text messages should not be sent from the primary line.

15.15 Emails and telephone messages (either verbal or text) which are, or may be considered to be, insulting, defamatory or libellous or which are contrary to the Council's Equal Opportunities policy are forbidden whether or not the person who is being insulted, defamed, libelled or discriminated against is likely to see the contents of the message.

15.16 Personal or confidential information should not be divulged over the telephone or by email without verifying the identity of the recipient independently.

15.17 Users must not use e-mail or telephones to publish confidential, critical or defamatory information about the Council or any other organisation or individual.

15.18 Sending emails or using a telephone in contravention of this policy may be considered gross misconduct and may result in summary dismissal for staff. Members contravening this policy may be referred to the Standards Committee.

15.19 The Council reserves the right to monitor the use of emails. telephones and the internet for the purposes of enforcing this policy in

accordance with the Telecommunications (Lawful Business) (Interception of Communications) Regulations 2000.

15.20 The Council undertakes regular monitoring of telephone and Internet usage via system generated reports. Senior Management is provided with regular reports on costs and times of calls and times and details of access to internet sites. Results from such monitoring may be used during a disciplinary investigation if such usage is outside the permissible uses outlined in this policy.

15.21 Should the Council be sued due to misuse of Council IM&T equipment or the actions of a user that contravene this policy, the Council reserves the right to claim damages from the user concerned.

16 All Staff Distribution List

16.1 Use of the All Staff distribution list is restricted to the following:

i) Urgent messages relating to work (for example: requests to find out who wants a particular invoice that has been received in the wrong division)

ii) Urgent messages relating to the Sports and Social Club activities (for example: advertising spare tickets for a social event)

iii) Messages from UNISON issued through the Branch Secretary

iv) Other messages must not be sent to all staff without the prior approval of a Head of Division or HR and IM&T.

16.2 General information to staff, Members and contractors, including advance notice of social events, should normally be given through City Voice or the Members Briefing Note and should be sent to the Council's Corporate Communications Manager.

16.3 Any person who has information that they feel should be distributed to all staff (for example: a warning about cheque fraud in the area) must speak to IM&T and the communications team who will check the information and issue a warning if appropriate. This is to ensure that those receiving messages are clear that they are genuine and not a hoax.

17 Internet Use

17.1 When using the Internet, chat rooms or bulletin boards, the following guidelines should be adhered to:

i) Job-related details from approved sites may be downloaded.

ii) Downloading of any program or update to programs must be done only by the Council's IT contractor because of the high risk of infecting a system with a virus, i.e. Microsoft updates.

iii) Downloading games or software to Council equipment is prohibited.

iv) Postings made to bulletin boards should not contravene Council policies nor damage the Council's reputation.

v) Loading of any information onto the Intranet or Internet that may be detrimental to the Council is prohibited.

vi) The Council will block any Internet site that is deemed unsuitable e.g. pornographic sites; it will also block any sites that are being used excessively during working hours. Access to sites will be authorised during lunch hours, before and after core hours.

18 Offensive, Illegal, Pornographic and Sexually Explicit Material

18.1 Offensive material is anything that is pornographic, involves threats or violence, and promotes illegal acts, racial or religious hatred, or discrimination of any kind. It also covers sending material which the person knows or ought to have known could offend colleagues or other recipients with particular sensitivities, even if it is not explicitly offensive, for example, religious or pro-hunting views.

18.2 Anyone using Council equipment for such material will face serious disciplinary action. If illegal material is accessed, the Council will inform the police and criminal action may follow.

18.3 Often when accessing a harmless site, links are automatically made to other sites or pages, and these could be inappropriate. Anyone accessing such sites accidentally should inform their manager immediately and IM&T. Accidental access may not result in disciplinary action, but failure to report it could do so.

18.4 People receiving offensive or sexually explicit material should inform their manager and IM&T immediately. Such material may not be identifiable until opened and, in these cases, individuals will not be held responsible provided they report it immediately.

18.5 People receiving hate mail or emails asking for money should refer these to IM&T immediately and HR should be informed.

18.6 Any user who accidentally encounters offensive material on the Internet, or who is sent offensive material via e-mail or any other means, or witnesses the accessing of offensive material must report the incident immediately to their Manager, HR and IM&T.

18.7 Individuals who bring their own laptops, other electronic devices or external storage devices into the workplace containing illegal or offensive material will be treated in the same way as those using Council equipment. Similarly, those who use their own equipment to connect to the Council's network remotely and who use that connection in this manner will be treated in the same way as those using Council equipment.

18.8 On occasion staff may need to access such sites in undertaking their duties, but before doing so they should obtain permission from their Manager or Head of Division and IM&T must be informed. Each site visited should be recorded in a log which identifies the site and the

date and time of the visit. The log will be reviewed regularly by the Head of Organisation Development and Head of IM&T

18.9 Except in these circumstances there can be no possible legitimate Council use for accessing or transmitting sexually explicit materials at work. The accessing, viewing, downloading, storing or printing of any content of an illegal, pornographic or sexually offensive nature is expressly forbidden and will be treated as gross misconduct leading to summary dismissal for staff or, for Members, to a report to the Standards Committee.

19 Government Connect

19.1 The Council are planning to implement Government Connect specifically GC Mail which is a centrally supported common solution with a reliable, robust, and secure way to send emails and attachments across government. Access to Government Connect will be restricted and all users must sign a 'Personal Commitment Statement'. The Personal Commitment Statement can be seen at Appendix B.

19.2 Any member of staff using Government Connect must undergo the Baseline Personnel Security Standard (BS), which is not a formal security clearance but provides a level of assurance to the trustworthiness and integrity and probable reliability of prospective and current employees.

19.3 A BS checks involves verification of:

- Identity
- Employment history (past 3 years)
- Nationality and immigration status
- Criminal Record (unspent convictions only)

All checks will be carried out through Organisational Development.

Appendix A – Glossary of Terms (Definition of terms and expressions used within this document)	
Bulletin Board	An area on the Intranet or Internet where people can share and publicise information and programs relating to their common interest.
Downloading	To transfer data, software or images from one computer to the memory of another device (e.g. smaller computer).
Electronic Systems	Fax machines; e-mail; voice mail; Internet; video conferencing; network, personal and laptop computers; mobile phones; pagers; text messaging; two-way radios; or other similar technology as may be available from time to time.
EDRM	Electronic Document and Records Management – a storage area for documents and records
End User/User	Anyone using a PC/laptop/phone.
E-mail	Message sent from an individual to one (or more) individuals or companies or bulletin boards electronically.
Executable code	A computer program that performs a task rather than just relaying a message or a set of data.
Freeware	Software that is licensed for use free of charge but with restrictions on use set by the software author(s).
Hacking	Gaining illegal access to a computer system. Abuse or security breach on any system or storage media.
IM&T	Information Management and Technology
Internet	A world wide network of computers following a recognised addressing convention so that sets of data on them are readily accessible to computer users.
Intranet	A model of the Internet, which is available only within a particular organisation – i.e. external access is not possible.
Licence	Authority from the software developer to use the software and specifying the use to which it may be put. A software licence will also specify the number of permitted concurrent uses of the software.
PDAs	Personal digital assistant such as a hand held personal organiser.

Personal Use	Use of Winchester City Council assets for personal (non profit) purposes. Examples may be typing a personal letter or browsing the Internet for non-work related purposes.
Personal Business	Activities relating to a private venture/business in which the employee has an interest whether financial or not.
Private Use	Use of Winchester City Council communication facilities for any calls other than emergency calls i.e. Needing to contact child minder, contact a family member.
Shareware	Software that may be used for evaluation purposes only until such times as it is registered and paid for.
Staff	Any person employed by the Council, either directly, on contract or volunteer/work experience.
USB	Universal serial bus – a standard connection method that connects an external device (such as a memory stick, joystick, camera, phone, mouse or keyboard) to a computer.
Users	Any person with access to any of the Council's systems. This will include all staff directly employed by the Council, as well as agency staff, contractors and elected Members.
Virus	Piece of software whose purpose is maliciously to alter the performance of a computer or the data that it holds. Many computer viruses are transmitted undetected alongside information or software that is wanted by the person putting it on their computer and can lie undetected until a trigger (such as a particular system date) causes it to be actioned. The effects can devastate computer installations.
World Wide Web	Graphical presentation of data on the Internet making it much more accessible and readily available to users.

Appendix B – Government Connect Personal Statement

Government Connect – Personal Commitment Statement

I understand and agree to comply with the security rules of Winchester City Council as well as the GSi Code of Connection (CoCo).

I acknowledge that my use of GSi may be monitored and/or recorded for lawful purposes:

I agree to be responsible for any use by me of the GSi using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address; and

Will not use a colleague's credentials to access the GSi and will equally ensure that my credentials are not shared and are protected against misuse; and

Will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at Winchester City Council's premises); and

Will not attempt to access any computer system that I have not given explicit permission to access; and

Will not attempt to access the GSi other than from the IT systems and locations which I have been explicitly authorised to use for this purpose; and

Will not transmit information via the GSi that I know, suspect or have been advised is of a higher level of sensitivity than my GSi domain is designed top carry; and

Will not transmit information via the GSi that I know or suspect to be unacceptable within the context and purpose for which it is being communicated; and

Will not make false claims or denials relating to my use of the GSi (e.g. falsely denying that an e-mail had been sent or received); and

Will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GSi to the same level as I would paper copies of similar material; and

Will not send Protectively Marked information over public networks such as the Internet; and

Will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain; and

Will not auto-forward email from my GSi account to any other non-GSi email account; and

Will disclose information received via the GSi only on a 'need to know' basis; and

Will not forward or disclose any sensitive or protectively marked material received via the GSi unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel; and

Will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received by GSi (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted; and

Will securely store or destroy any printed material; and

Will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the GSi (this might be by closing the e-mail program, logging off from the computer, activate a password protected screensaver, etc, so as to require a user logon for activation); and

Where Winchester City Council has implemented other measures to protect unauthorised viewing of information displayed on IT screens (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection; and

Will make myself familiar with the security policies, procedures and any special instructions that relate to GSi; and

Will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security; and

Will not attempt to bypass or subvert security controls or to use them for any purpose other than that intended; and

Will not remove equipment or information from Winchester City Council's premises without appropriate approval; and

Will take precautions to protect all computer media and portable computers when carrying them outside Winchester City Council premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief); and

Will not introduce viruses, Trojan horses or other malware into the system or GSi; and

Will not disable anti-virus protection provided at my computer; and

Will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that Winchester City Council informs me are relevant; and

If I am about to leave Winchester City Council, I will inform my manager prior to departure of any important information held in my account.

Signed Date